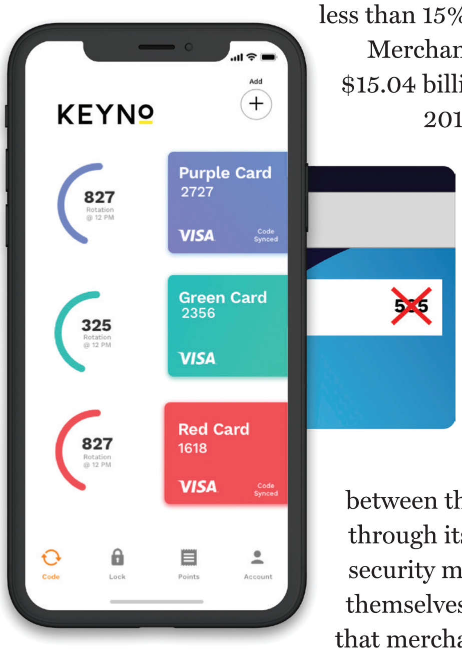
THE NILSON REPORT

FOR 49 YEARS, THE LEADING PUBLICATION COVERING PAYMENT SYSTEMS WORLDWIDE JANUARY 2020 / ISSUE 1167

CNP Fraud Prevention for Issuers



Issuers, merchants, and acquirers that process card payments from their merchant customers spend heavily to protect themselves from card-not-present (CNP) fraud, which accounts for 54% of all fraud losses even though CNP purchases account for less than 15% of all sales billed to cards.

Merchants incurred nearly all of the $15.04 billion in CNP fraud losses in 2018. However, issuers can help them by using technology from Keyno, which prevents CNP fraud through the use of dynamic card verification value (dCVV2) numbers stored in the cloud and made available on a mobile phone to be entered at the time of an online purchase. The difference between the security Keyno offers issuers through its CVVkey service and the security merchants deploy to protect themselves, including 3D Secure 2.0, is that merchants aim to detect fraud as it occurs, using a risk scoring model. Keyno's technology prevents the possibility of fraud from occurring by blocking authorization attempts.

In collaboration with Visa, Keyno will work with issuers to deploy CVVkey in any country in which VisaNet handles card payments. Through an API with VisaNet, Keyno registers cards for dCVV2 and provides the cardholder with CVVkey. VisaNet holds the Visa primary account number (PAN) and the current dynamic CVV2 codes. It validates the dCVV2 code and passes that information on to the issuer.

When authorizations are approved, the merchant only sees a dynamic CVV2, which, if stolen, could never be used to gain a valid authorization for any other transaction. There is no need for an issuer's card account processor to make any system changes.

Issuers will give cardholders the option to participate. Keyno will supply an SDK plug-in that issuers can use to add the opt-in service to their mobile app or they can offer Keyno's app on a white-label basis. It takes less than a minute for a cardholder to register. When they make an online payment they need to have their phone in-hand to view the code.

Initial opportunities for Keyno include the U.S. (for credit cards only), Canada, the U.K., France, and select markets in Asia-Pacific and the Middle East.

Keyno says it can install its technology at any issuer in 6 to 8 weeks. It expects to be live with its first customers by the end of the second quarter of this year.

PSD2, the payment regulation in place in Europe since June 2019, requires that two or more elements be in place for authorizations to be valid. Those elements include something the user knows (knowledge), something only the user possesses (possession), and something the user is (inherent). Keyno says its technology meets PSD2 requirements.

No need for card account processors to make any system changes.

Visa will be the first network to support Keyno. However, it does not have an exclusive.

An advantage of Keyno's dynamic CVV2 versus dynamic CVV2 codes available from card manufacturers that embed the technology in a payment card and display it on a screen is that issuers can deploy CVVkey on cards already in circulation. It can be deployed on an individual cardholder basis or on a card-by-card basis—a choice made by cardholders.

Robert Steinman is Chief Executive Officer at Keyno in Laguna Beach, California, robert@keyno.io, www.keyno.io.

Posted with permission from
The Nilson Report, Carpinteria, California.
Click here to learn more about the publication.